

**12 M 440**JP:MKM  
F.#2012R00468UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- x	
UNITED STATES OF AMERICA	: TO BE FILED UNDER SEAL
	:
- against -	: COMPLAINT AND AFFIDAVIT
	: IN SUPPORT OF APPLICATION
JORGE MORANTE,	: <u>FOR ARREST WARRANT</u>
also known as	:
"Manuel Daniero,"	: (18 U.S.C. § 1343)
	:
Defendant.	:
----- x	
----- x	
IN THE APPLICATION OF THE UNITED	: AFFIDAVIT IN SUPPORT OF
STATES OF AMERICA TO SEARCH THE	: <u>SEARCH WARRANT</u>
PREMISES KNOWN AND DESCRIBED AS	:
201-17 53rd AVENUE, OAKLAND	: (18 U.S.C. § 1343)
GARDENS, NEW YORK 11365	:
----- x	

EASTERN DISTRICT OF NEW YORK, SS:

BRIAN COLICA, being duly sworn, deposes and states that he is a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, on or about and between April 2005 and May 3, 2012, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant JORGE MORANTE did knowingly and willfully devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, and did unlawfully,

willfully and knowingly transmit and cause to be transmitted by means of wire communication in interstate commerce, signs, signals and sounds for the purpose of executing such scheme and artifice to defraud, to wit: the defendant, through the use of telephones in Queens, New York, called DirectTV and activated numerous DirectTV receivers under false pretenses, and then sold the use of the activated receivers to others.

(Title 18, United States Code, Section 1343)

Also upon information and belief, there is probable cause to believe that there is located within the premises known and described as 201-17 53rd AVENUE, OAKLAND GARDENS, NEW YORK 11365 ("SUBJECT PREMISES"): documents, books and records, including electronic files on computers, as described with more particularity in Attachment A, that constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343.

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with HSI for approximately two-and-a-half years and am currently assigned to the El Dorado Task Force where my work includes the investigation and prosecution of mail and wire fraud. I have participated in the investigation of this matter, and I am familiar with the information contained in this Affidavit based on my own personal

participation in the investigation, my review of documents, and conversations I have had with other law enforcement agents, DirecTV representatives, and other individuals. Because this Affidavit is being submitted for the limited purpose of obtaining arrest and search warrants, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

2. An HSI investigation has revealed that JORGE MORANTE ("MORANTE"), together with others, is executing a "mirroring" scheme involving the following aspects:

3. DIRECTV (DTV) is a provider of digital television services, which provides access to television programs through the use of a receiver connected to the customer's television. A residential customer may request additional receivers to be used with additional televisions throughout the residence for a fee of \$6.00 for each additional receiver on the account. Under this arrangement, DTV "mirrors" the programming to the additional televisions within the residence. Under DTV's customer agreement, all active receivers on a single residential account must be located and used in within the residence associated with the account and customers agree to provide true and accurate information about the location of their receivers. In a

mirroring fraud, numerous receivers are activated on a single residential account, but the receivers are actually located in other residences. In this way, the perpetrators obtain the DTV services for \$6.00 for each additional location, rather than the full price of the DTV services.

4. Automatic number identification (ANI) enables DTV to identify the telephone number of the customers who call in to activate an account or request additional receivers. The investigation has revealed that the telephone number 718-423-6268 (the "6268 number") has been used to maintain and inquire about 81 separate DTV accounts. A second telephone number, 917-662-0494 (the "0494 number") has also been used with regard to several of the same accounts as well as some additional accounts. In total, the 6268 number and the 0494 number have been used in maintaining and inquiring about 85 accounts.

5. A records check revealed that the 6268 number is in use by MORANTE at the residence of the SUBJECT PREMISES and the 0494 is MORANTE's cellular telephone. In an application for a U.S. passport, a female applicant listed MORANTE as her emergency contact and indicated that he lives at the SUBJECT PREMISES and uses the 6268 number. In an application for a U.S. passport, another female applicant identified MORANTE as her father and her emergency contact, and indicated that he lives at the SUBJECT PREMISES and uses the 0494 number.

6. The DTV accounts associated with the 6268 and 0494 numbers were activated through DTV dealers. Of the 85 accounts associated with those two numbers, 42 were activated by DTV dealership Rampergi Inc., located in Kissimmee, Florida. When interviewed, the owner of Rampergi stated that MORANTE created the 42 accounts activated through Rampergi that are associated with the 6268 and 0494 numbers and provided his address as the SUBJECT PREMISES.

7. During the initial account activation, MORANTE activated only one or two receivers per account. Thereafter, MORANTE added additional receivers onto the accounts. There was an average of eight receivers per account, including two accounts with as many as twelve active receivers. For the 85 accounts associated with the 6268 and 0494 numbers, there are a total of 692 active DTV receivers in use.

8. For the 85 accounts associated with the 6268 and 0494 numbers, payments to DTV have been made from two J.P. Morgan Chase checking accounts with account numbers ending 6465 and 6875 ("CHASE CHECKING ACCOUNTS"). Both CHASE CHECKING ACCOUNTS are registered to "Concordia Enterprises Inc." at the SUBJECT PREMISES. A Chase credit card account with account number ending 2037 ("CHASE CREDIT CARD") is in the name "Jorge E Morante, Concordia Enterprises" at the SUBJECT PREMISES. Concordia Enterprises Inc. is not an authorized provider of such services.

9. Account statements for the CHASE CHECKING ACCOUNTS show that numerous check deposits are made into the accounts each month ranging from \$20 to \$130 in addition to numerous cash deposits. Images of the checks and deposit slips for many of the deposits into the CHASE CHECKING ACCOUNTS show that the checks and cash deposits are made out to Concordia Enterprises or MORANTE for various amounts of money.

10. Social security numbers and/or other personally identifiable information was provided upon the opening of the 85 accounts associated with the 6268 and 0494 numbers. However, many of the social security numbers do not match records of the names and/or addresses of the individuals properly assigned those social security numbers.

11. Based on the criminal history report of the defendant JORGE MORANTE, the defendant is a Hispanic male who is 49 years old, 5'11" tall, and weighs 150 pounds. MORANTE is a legal permanent resident in the United States and a photograph in MORANTE's A-file confirms this description. MORANTE's criminal history also indicates that he was previously convicted in this district of credit card fraud under the name "Manuel Daneiro."

12. The TARGET PREMISES is further described as a two-story private house located on the corner of 53rd Avenue and 202nd Street in Oakland Gardens, Queens, New York. The TARGET PREMISES has white siding, a small covered entryway and multiple

satellite dishes on top of the house. To the right side of the steps up to the front door, when facing the SUBJECT PREMISES, is a bay window. The number "201-17" is displayed on the front of the house.

13. I observed MORANTE entering and leaving the SUBJECT PREMISES on several occasions, most recently on April 25, 2012. In addition, a credit card statement for the CHASE CREDIT CARD for the period ending April 14, 2012 indicates that the account is currently in the name "Jorge E Morante, Concordia Enterprises" at the SUBJECT PREMISES.

14. Based on the information set forth in this Affidavit, there is probable cause to believe that there are evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343 as set forth in Attachment A located within the SUBJECT PREMISES.

15. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, in whatever form they are found. I submit that if a computer or electronic medium is found on the premises, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

A. Based on my knowledge, training, experience, and information related to me by agents and others involved in

the forensic examination of computers, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

C. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.



D. Based on actual inspection of credit card statements, I am aware that computer equipment was used to make payments on the account of the CHASE CREDIT CARD in the name of "Jorge E Morante, Concordia Enterprises" at the SUBJECT PREMISES as part of the mirroring scheme. There is reason to believe that there is a computer system currently located on the SUBJECT PREMISES.

16. Because multiple people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

17. Based upon my knowledge, training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and

completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

A. The volume of evidence. Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

B. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting

scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

18. In light of these concerns, I hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

19. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using

key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, HSI intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for defendant JORGE MORANTE, also known as "Manuel Daneiro" so that he may be dealt with according to law.

WHEREFORE, your deponent respectfully requests that a search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 201-17 53rd AVENUE, OAKLAND GARDENS, NEW YORK 11365 to search and to seize documents, books and records, including electronic files on computers, as described with more particularity in Attachment A, that constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343.

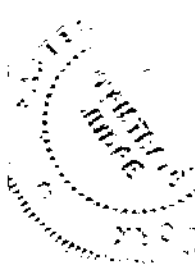
Because this investigation is ongoing, and in light of the nature of this Affidavit, it is further respectfully

requested that this Affidavit and Application and any Order issued thereon be ordered sealed until further notice.



BRIAN COLICA  
Special Agent  
U.S. Department of Homeland Security,  
Homeland Security Investigations

Sworn to before me this  
3rd day of May, 2012



HONORABLE ROBERT M. LEVY  
United States Magistrate Judge  
Eastern District of New York

**ATTACHMENT A: Evidence to be Seized**

Evidence to be seized, all of which constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343.

- (A) Financial documents dated on or after April 2005, including, but not limited to, money orders, checks, bank statements, credit card account records, deposit receipts and currency transactions records.
- (B) Records, receipts, statements, books, logs, ledgers, lists, and any other documents revealing information relating directly or indirectly to Concordia Enterprises Inc. and/or DirecTV.
- (C) Records, books, logs, ledgers, lists, and any other documents containing personally identifiable information, including but not limited to names, social security numbers, dates of birth and addresses associated with individuals other than Jorge Morante.
- (D) Computer hardware, meaning any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
- (E) Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation

of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

- (F) Computer-related documentation, meaning any written, recorded, printed, or electronically-stored material which explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- (G) Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.
- (H) Any computer or electronic records, documents, and materials, including those used to facilitate interstate communications, in whatever form and by whatever means such records, documents, or materials, their drafts or their modifications, may have been created or stored, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly, relating to the described offense); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
- (I) Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form such information might take

includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

- (J) Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data, in the form of electronic records, documents, and materials, including those used to facilitate interstate communications. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.
- (K) Records of personal and business activities relating to the operation of a computer, such as telephone records, notes (however and wherever written, stored or maintained), books, diaries, and reference materials relating to the described offense.
- (L) Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.
- (M) Any safes or safe-deposit boxes.
- (N) Cellular telephones used by JORGE MORANTE, including but not limited to the cellular telephone with the 0494 number, as defined in the Affidavit.